UNITED STATES DISTRICT FOR THE
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,
v.

JOHN STUART,

Defendant.

21-CR-07-LJV-JJM

MEMORANDUM/BRIEF

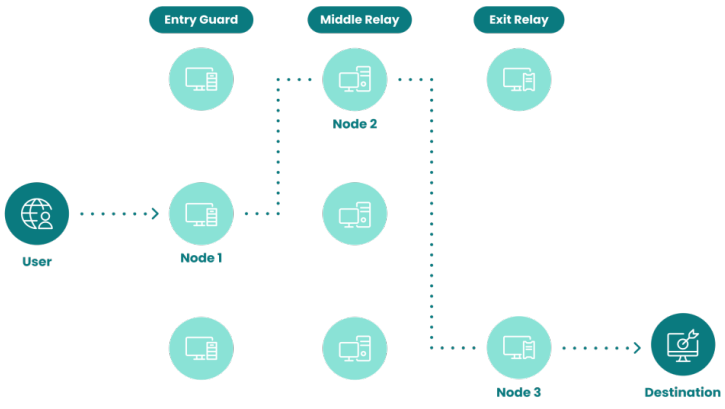
At oral argument on Mr. Stuart's motion to compel (Docket No. 49), this Court set a deadline for the government to make further disclosures and ordered that the defense file a brief identifying whether, and to what extent, the government's additional production resolves the discovery sought in the motion to compel. The government has since provided an unredacted copy of a complaint in a separate but related matter pursuant to the defense's request. Accordingly, that matter has been resolved.

The government also composed a letter to the defense to "provide additional information" regarding the background of the investigation that led to the search of Mr. Stuart's home. The government asserts in the letter that the information it contains is "neither discoverable, nor relevant to any material issue" but is provided to "clarify protentional misunderstandings."

The defense disagrees with the characterization that the information provided in the letter, as well as other still outstanding discovery, is neither relevant nor discoverable. To the contrary, since this information pertains to the manner and method in which a search warrant was obtained to search Mr. Stuart's home, it is both deeply relevant and discoverable. In fact, this information should have been previously disclosed not only to the defense, but more importantly to the issuing-magistrate judge at the time of the warrant application.

The government now claims that one foreign law enforcement agency (FLA) seized the server at issue and another FLA deanonymized the IP addresses provided to them by the first FLA.[1] The second FLA, according the government in its letter, "did not disclose to the United States the methodology it used" to uncover the defendant's IP address. In practice, this suggests that by seizing and searching the server (the IP address of which was first identified by the United States government) the first FLA acquired IP address logs of visitors and the second FLA used a yet-to-be identified method to deanonymize the true IP address.

This requires some explanation. Because the website at issue in this case is hosted by a server on the Tor network, the IP address logs uncovered by the first FLA would be worthless. They would likely represent simply the "exit node" IP address, the last in chain or "onion" of IP addresses that are used to route the request to visit the website. Through this method, Tor can achieve its goal of anonymizing the true user IP's address. To discover where the request to visit a website actually originated, the second FLA would have had to peel back the layers of the onion, or trace the IP addresses through various relay points all the way back to the original user. Below is a graphical illustration of this concept:



[1] The FLAs at issue are the subject of a protective order but are known to the parties and the Court. The government's letter, also subject to the order, will be provided to the Court and docketed as a sealed exhibit.

Here, the user requests a website identified in the illustration as a "destination." That request is then encrypted and routed through various nodes so that the destination site does not know the original or true user's IP address.

It is this method of unencrypting and tracing back, or unpeeling the union, that the government now claims it is not privy too, and/or does not want to disclose.

But this is the whole ball of wax. Lacking any transparency in this part of the process, it is impossible to know whether whatever method the second FLA used was a reliable and accurate one. This is especially true given the government's assertion that a NIT[2] was not used. This means that some other new, yet-unknown, potentially untested technique was used. This Court does not know, and the issuing magistrate judge could not have known, the reliability of this technique. To put it bluntly, based on the government latest revelations, there is simply no way to know if the IP address that the second FLA said visited the website *actually visited* the website. The mystery technique might have gotten it wrong. The mystery technique might have identified Mr. Stuart IP's address when it was actually Mr. Smith's, or one of the other millions of IP addresses in the world that visited the site.

The government's effort to explain itself is both too little and too late. In the defense's reply, the defense requested:

- All the foreign law enforcement agencies (FLA) and countries involved in all aspects of the investigation.
- What role each FLA had.
- U.S. law enforcement's full role, including what techniques were utilized and when they were utilized.

[2] A NIT or Network Investigation Technique is simply a label the government uses to describe the malware it has installed on American's computers. In the Playpen investigation, for instance the NIT used by the government was malware that was surreptitiously disseminated through a Tor hidden service. The malware was designed to pierce the anonymity provided by the Tor network by placing computer code on users' computers that would transmit private information back to a law enforcement server outside of the Tor network.

- Which U.S. agencies were involved and how.
- All information and documentation related to Project Habitance in the possession of the prosecution team, as that term is defined by caselaw.
- What technique was used to locate, take down and seize the server.
- What technique was used to de-anonymize the website's IP address.
- Whether Mr. Stuart had account on the website in question.

While the government's letter attempts to answer some of these requests with a narrative, the government has still not provided any documentation or data relative to the requests. Moreover, as the government itself would certainly admit, the prosecutor in this case has no first hand knowledge of any of the information detailed the letter. It simply represents a hearsay account of an investigation from the government's point of view. Critically, no documents or information have been provided regarding the technique or techniques used to deanonymize the IP addresses that purportedly led to the one associated with Mr. Stuart. Without this crucial information, the government can make no assurance on the reliability or constitutionality of that process. Indeed, there are "two circumstances where evidence obtained in a foreign jurisdiction may be excluded: first, where the conduct of foreign officials in acquiring the evidence is so extreme that it shocks the judicial conscience and second, where cooperation with foreign law enforcement officials may implicate constitutional restrictions." *United States v. Getto*, 729 F.3d 221, 228 (2d Cir. 2013). If the government cannot tell this Court that how the evidence was gathered, it cannot assure this Court that it does not shock the conscience. Nor can the government assure this Court now, nor the issuing magistrate then, that the process – a process it claims to know nothing about – was a reliable

one.

Accordingly, this Court should compel the government to disclose materials identified above, as well as the methodology used to deanonymize the IP addresses.

Further, in the defense's reply to the motion to compel, the defense noted that it anticipated filing further motions based on what was, or was not, disclosed as a result of the motion. Based on what we know now, this Court should also set a *Franks* hearing.

In *Franks v. Delaware*, the Supreme Court held that a defendant is entitled to a hearing to challenge the truthfulness of statements in a search warrant affidavit if he makes "a substantial preliminary showing" that the statements were "knowingly and intentionally [false], or [made] with reckless disregard for the truth," and that the falsehood was "necessary to the finding of probable cause." *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). The right to a *Franks* hearing is triggered not only by false statements but also by material omissions. When a defendant alleges a material omission has been made, [t]he required showing is two-fold: first, the omission must have been either intentional or reckless; and second, the omitted information, if incorporated into the affidavit, must be sufficient to vitiate probable cause.

Task Force Officer Hockwater made omissions and misstatements knowingly and intentionally, or with reckless disregard for the truth, regarding four key issues. First, Hockwater made material misstatements about the nature, origin, and reliability of the tip from the FLA. Second, Hockwater made material omissions about the method(s) used by the FLA to identify the IP address. Third, Hockwater's explanation of Tor was misleading. Fourth, Hockwater misrepresented the relationship between U.S. law enforcement and the FLA(s) in the affidavit. Each of these misstatements and misrepresentations went directly to the heart of the probable cause analysis. The magistrate would not have issued the warrant had these

misrepresentations been corrected in the affidavit because the reformed affidavit would not establish probable cause.

Second, this Court should re-open the previously-filed motion to suppress. When an affidavit relies on information provided by a confidential informant, the affidavit must provide some information from which a magistrate can credit the informant's credibility. Here, the affidavit submitted in support of the search warrant failed to establish a "fair probability" that evidence of a crime would be found in Mr. Stuart's home. *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983). The affidavit relied entirely on an unsubstantiated allegation of criminal activity by an unidentified foreign law enforcement agency (now known). The affidavit failed to include any information as to how the second FLA came across that information, how reliable the method the second FLA used to obtain the information was (if indeed it was that FLA that deanonymized the suspect user IP address here), and whether the IP address and/or other tip information was obtained through the second FLA's first-hand knowledge or through other sources.

Although this Court has issued a Report and Recommendation declining to suppress on the basis of unreliability (Docket No. 33, *adopted*, Docket No. 44), this new information completely changes the landscape. The defense learned for the first time that the second FLA used an unknown technique to deanonymize the IP addresses in the government's letter provided only weeks ago, years into the case against Mr. Stuart. This new information firmly underscores that the blanket assertion in the search warrant application – that the second FLA has provided "accurate and reliable information" in the past – is so broad and vague as to be meaningless. The warrant affidavit does not, and seemingly cannot, make any assurance as to the reliability of the method used to produce the IP address in this case. The affidavit does not

even specify whether the second FLA's purported previous reliability has anything to do with the subject area at issue in this case. For all we and the issuing magistrate know, the second FLA has provided accurate tips about the whereabouts of suspects on the run, or drug dealers' selling habits. This would have no bearing on the issuing-magistrate's confidence in the manner in which the tip in this case was generated, and tellingly no assurances whatsoever on that score are provided.

We also now know that this assertion did not even come from Hockwater's own personal knowledge, but rather from a stock application that Hockwater simply passed on to the issuing-magistrate judge as a middleman. In other words, the sworn assertion that this Court based its Report and Recommendation on – that the second FLA has provided accurate and reliable information in the past – did not even come from Hockwater himself. Accordingly, this Court should re-open the motion to suppress.

Dated: Buffalo, New York
March 1, 2023

Respectfully submitted,

/s/ Jeffrey T. Bagley
Jeffrey T. Bagley
jeffrey_bagley@fd.org
Assistant Federal Public Defenders
Federal Public Defender's Office
300 Pearl Street, Suite 200
Buffalo, New York 14202
(716) 551-3341